

IT-Security Policy nach internationalem Standard

Wege zu einem proaktiven Risikomanagement und einer modernen IT Governance im gewerblichen Mittelstand, in Behörden und in der öffentlichen Verwaltung

Autoren: Rudolf Gelhaus, Geschäftsführender Gesellschafter
Günter H. Hirschmann, Gesellschafter der Neupart GmbH, Bad Driburg

1 Einleitung

Wenn kritische Geschäftsprozesse durch infrastrukturelle Störungen der IT und Informationsverarbeitung beeinträchtigt werden, so sind oftmals längere Ausfallzeiten die Folge. Diese operationellen Risiken können entstehen, sobald ein Unternehmen externen Einflüssen unterliegt oder Mitarbeiter bzw. Systeme in Prozesse einsetzt. Wie die Erfahrungen der letzten Jahre zeigen, stellen operationelle Risiken eine wesentliche Quelle finanzieller Verluste dar. Bei genauerer Betrachtung steht ein erheblicher Anteil der Schadensfälle, die in Unternehmen auftreten, im Zusammenhang mit dieser Risikokategorie. Inkompetenz, verbrecherische Neigungen, Ausscheiden oder Ausfall von Mitarbeitern, diverse Prozessfehler (Buchung, Abwicklung, Bewertung), Ausfälle technischer Systeme sowie Gefahren, die von externen Faktoren, wie Gewalt und Wirtschaftskriminalität, physischen Bedrohungen bzw. Naturkatastrophen, bis hin zu den Rechtsrisiken ausgehen, haben somit ein entsprechendes Wirkungspotenzial. Der wichtigste Block der operationellen Risiken sind jedoch die IT-Risiken.

Wenn es darum geht, eine effektive IT-Sicherheitsrichtlinie zu formulieren und umzusetzen sowie die Mitarbeiter in diesem Bereich zu schulen, liegen mittelständische Betriebe gegenüber den Großunternehmen noch immer weit zurück¹. Dennoch: Immer mehr Manager sind sich ihrer Verantwortung für die IT-Sicherheit im Unternehmen bewusst. Denn wer seine Firmen-IT nicht ausreichend schützt, handelt fahrlässig. Im Schadensfall werden Führungskräfte auch persönlich haftbar gemacht. Vorstandsmitglieder und Aufsichtsräte von Aktiengesellschaften, aber auch Geschäftsführer von kleineren Unternehmen sehen sich bekanntlich in zunehmendem Maße Rechts- und Haftungsrisiken ausgesetzt. In den letzten Jahren sind die Verhaltensanforderungen an Organmitglieder im Gefolge neuer Gesetze und gerichtlicher Leitentscheidungen präzisiert und teilweise erheblich verschärft worden.

2 Rechts- und Haftungsrisiken

Der Gesetzgeber hat mit gesteigerter Aufmerksamkeit den Rechtsbereich der Haftung von Organmitgliedern einer Gesellschaft ins Visier genommen². Die Jahre 2004 und 2005 standen ganz im Zeichen der Umsetzung des Maßnahmenkatalogs zur Stärkung der Unternehmensintegrität und des Anlegerschutzes („10-Punkte-Programm“ der damaligen rot-grünen Bundesregierung vom 25. Februar 2003³). Anfang Juli 2005 passierten zwei bedeutende Gesetze den Bundesrat: Das Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) und das Kapitalanlegermusterverfahrensgesetz (KapMuG).⁴ Durch das UMAG, das am 1. November 2005 in Kraft getreten ist,⁵ wird sich aller Voraussicht nach das Risiko für Vorstände und Aufsichtsräte deutlich erhöhen, von Minderheitsaktionären wegen Pflichtverletzungen auf Schadensersatzzahlungen an die Gesellschaft in Anspruch genommen zu werden. Ohnehin ist die Tendenz erkennbar, Haftungsansprüche im-

¹ Siehe z.B. Ernst & Young Best Practices Survey "Risikomanagement 2005", Köln 2005.

² Jetzt zusammenfassend Winfried F. Schmitz/Judith Rübenkönig: Haftung von Vorständen und Aufsichtsräten, in: Rechts- und Haftungsrisiken im Unternehmensmanagement, hg. von Stefan Hirschmann/Frank Romeike, Köln 2006, S. 11ff.

³ Eine Zusammenfassung dieses 10-Punkte-Programmes ist im Internet unter der URL www.bmj.bund.de abrufbar.

⁴ Beschlüsse des Bundesrates vom 8. Juli 2005, BR-Drs. 454/05; Beschluss vom 8. Juli 2005, BR-Drs. 455/05.

⁵ BGBl. I 2005, S. 2802 (2808).

mer öfter geltend zu machen und durchzusetzen. Zwar bietet die gleichzeitige Kodifizierung eines größeren unternehmerischen Ermessensspielraums von Geschäftsführern (*Business Judgment Rule*) in § 93 Abs. 1 AktG, formal betrachtet, mehr Schutz für Vorstände und Aufsichtsräte. Anders als im US-amerikanischen Recht müssen die Vorstände indessen in aller Regel im Streitfall beweisen, dass sie keine Pflichtverletzungen begangen haben⁶. Für AGs ist dies ausdrücklich vorgeschrieben (§ 93 Abs. 2 AktG), für den GmbH-Geschäftsführer hat dies der Bundesgerichtshof (BGH) bereits im November 2002 festgestellt⁷. Auch der Aufsichtsrat einer AG muss sich davon überzeugen, dass die erforderlichen Maßnahmen im Rahmen des Risikomanagements durch den Vorstand ergriffen wurden⁸.

Zumindest teilweise lassen sich finanzielle Haftungsrisiken durch Haftpflichtversicherungen für Organe absichern, so genannte Directors and Officers Liability Insurance (D&O). Teilten sich vor zehn Jahren noch zwei U.S.-amerikanische Versicherer dieses Marktsegment, kommen nun auch deutsche Versicherer mit eigenen Policen auf den Markt. Mittlerweile dürfte fast jede börsennotierte Aktiengesellschaft in Deutschland für ihre Organe eine D&O-Deckung abgeschlossen haben, doch auch die Nachfrage bei nicht börsennotierten Aktiengesellschaften sowie bei GmbHs ist weiter ungebrochen. Zudem erhält der Vertrieb von D&O-Versicherungen insbesondere durch die Nachfolgesituation bei Gesellschafter-Geschäftsführen auf Fremdgeschäftsführer bei mittleren und kleinen Kapitalgesellschaften zunehmend Rückenwind. Gleichwohl entbindet der Abschluss einer solchen Versicherung nicht von allen Sorgen, denn insbesondere bei den versicherten Personen und den versicherten Gefahren können erhebliche Unterschiede bestehen, die eine Prüfung von Haftungsausschlüssen unerlässlich machen. Außerdem entbinden D&O-Versicherungen Manager nicht von ihrer strafrechtlichen Verantwortung und der Pflicht, sich über aktuelle Entwicklungen im Unternehmen zu informieren. Während spektakuläre Fälle wie EM.TV, Informattec oder Mannesmann im Blickfeld der Öffentlichkeit aufbereitet wurden, vollziehen sich gerichtliche Auseinandersetzungen um mögliches Fehlverhalten von Managern und den daraus resultierenden Schadenersatzforderungen meist unbeachtet einer größeren Medienaufmerksamkeit. Vorausschauende Vorbeugemaßnahmen gilt es deshalb, auch im Management von IT-Risiken zu ergreifen, zumal die Mehrzahl der Unternehmen weltweit heute davon ausgeht, dass ihnen durch Cyberkriminalität höhere Kosten entstehen als durch die physische Kriminalität. Hauptursachen für Umsatzeinbußen sind dabei insbesondere Verluste bestehender und potenzieller Kunden sowie Einbußen bei der Produktivität von Mitarbeitern⁹.

3 Banken als Wegweiser

Auch Banken und andere Finanzdienstleister sind darum bemüht, die IT-Sicherheit stärker ins Bewusstsein von Unternehmen zu rücken und wirken neben Kunden, Partnern und Handelsorganisationen als Triebfeder. Kreditinstitute, die auf Grund der weltweiten Verknüpfung ihrer Systeme besonders anfällig für Attacken von Hackern sind, haben sich des Problems bereits vor Jahren angenommen haben. Die systemtechnischen Sicherheitsvorkehrungen bedürfen aber nicht zuletzt wegen der hohen Sensibilität der Daten einer permanenten Weiterentwicklung. Schon heute ergeben sich aus einer Reihe von gesetzlichen Regelungen im Bankenbereich (Basel II, MaRisk usw.) weitreichende Anforderungen an das Risikomanagement und die Sicherheit der Informationsverarbeitung. Basel II verlangt gar explizit eine Hinterlegung operationeller Risiken mit Eigenkapital¹⁰. Und Risiken, die sich aus der Nutzung moderner Informationstechnologien ergeben, gelten als zentraler Bestandteil der operationellen Risiken. Da die Informationstechnologie heute in vielen Fällen die Geschäfts-

⁶ Vgl. Schmitz/Rübenkönig, Haftung von Vorständen und Aufsichtsräten, S. 13ff.

⁷ Urteil des BGH vom 4. November 2002, Az. II ZR 224/00.

⁸ Urteil des BGH vom 21. April 1997, Az. II ZR 175/95

⁹ Dies geht aus einer aktuellen Umfrage hervor, die im Auftrag von IBM bei Unternehmen weltweit in 17 Ländern, darunter in 8 europäischen Ländern, durchgeführt wurde. Gemäß der IBM-Studie, bei der mehr als 3.000 CIOs und IT-Verantwortliche befragt wurden, sind 84 Prozent der IT-Executives überzeugt, dass organisierte kriminelle Gruppen über das nötige technische Know-how verfügen, um in der Welt des Cybercrime zunehmend an die Stelle des einsamen Hackers treten.

¹⁰ Frank Romeike: Operationelle Risiken: Die ältesten Risiken der Welt, in: RiskNEWS, 01/2004, S. 16-17; Ders., Lexikon Risiko-Management, Köln 2004, S. 88.

prozesse der Banken vollständig determiniert, sind Risiken in der IT-Sicherheit aus Sicht der operationellen Risiken wohl die größten Risiken überhaupt, denen sich eine Bank ausgesetzt sieht. Eine gewisse Sensibilität für IT-Risiken verlangen die Kreditinstitute vor diesem Hintergrund auch von ihren Firmenkunden, was insbesondere im Rahmen des internen Ratingprozesses Relevanz erlangt.

4 Management von IT-Risiken und IT-Governance

Vorbeugen heißt in diesem Fall, eine dokumentierte IT-Sicherheitsrichtlinie mit Regeln und Verfahren zu entwickeln, die insbesondere alle Mitarbeiter auf IT-Security verpflichtet und die regelmäßig aktualisiert wird. Zwar ist die IT-Sicherheitsorganisation noch immer das Stiefkind vieler Unternehmen und ist das Bewusstsein für IT-Risiken weithin unterentwickelt¹¹, doch ist langsam ein Umdenkungsprozess und zunehmende Sensibilität für das Management von IT-Risiken erkennbar.

Vor diesem Hintergrund gewinnt vor allem die IT-Governance zunehmend an Bedeutung. IT-Governance umfasst dabei primär Management, Organisationsstruktur und Prozesse, die sicherstellen, dass die Unternehmensstrategie und deren Ziele durch die IT unterstützt werden. Kernsystem der IT-Governance ist ein Informationssicherheitsmanagementsystem (ISMS), das sich parallel zum klassischen Informationsmanagementsystem (IMS) etabliert hat. Ein ISMS hat die Aufgabe, die Sicherheit arbeitsteiliger und unternehmensübergreifender Geschäftsprozesse aufgrund möglicher Fehler und Schäden hinsichtlich des Zielniveaus in allen relevanten Dimensionen der Sicherheit festzulegen und die Erreichung dieser Ziele mittels geeigneter Vorgaben, Konzepte, Architekturen und operativer Maßnahmen sicherzustellen. Mithilfe von Kontrollen können Zielabweichungen durch externe oder interne Umstände erkannt und Gegenmaßnahmen ergriffen werden. Auf der strategischen Ebene erfolgt dabei die langfristige Festlegung der Ausrichtung des Informationsmanagements. Entsprechend seiner Bedeutung als Informationsversorgungssystem für ein Unternehmen fallen hierunter Aufgaben wie strategische Situationsanalyse, strategische Zielplanung und Strategieentwicklung für die Erreichung definierter Ziele. Die Aufgaben der administrativen Ebene werden dagegen als taktische Aufgaben bezeichnet und unmittelbar aus den Ergebnissen der strategischen Planung abgeleitet. Auf dieser Ebene erfolgt beispielsweise ein erster Teil der Umsetzung der IT-Fachaufgabe sowie die Vertragsgestaltung mit den Abnehmern von IT-Leistungen. Ebenso dient die administrative Ebene zur Informationssystemplanung und Informationssystementwicklung. Auf der operativen Ebene wird die Nutzung vorhandener Infrastruktur gemanagt¹².

Trotz aller Komplexität: Eine unternehmensbezogene ganzheitliche Sicherheitsrichtlinie zu erstellen, diese kontinuierlich zu pflegen und die Mitarbeiter zielführend in IT-Sicherheit zu unterrichten, ist mittlerweile keine exklusive Domäne der großen Industrieunternehmen mehr. Wichtig ist aber für kleinere Unternehmen und öffentliche Einrichtungen – insbesondere vor dem Hintergrund der beschriebenen Rechts- und Haftungsrisiken –, dass die meist mit Hilfe von Softwareprogrammen unterstützten Security Policies den international anerkannten Standards wie British Standard BS 7799-2¹³ bzw. inzwischen ISO/IEC 27001¹⁴

¹¹ Vgl. KES/KPMG-Sicherheitsstudie, Ingelheim 2002.

¹² Vgl. Wolfgang J. Böhmer: IT-Governance als Erfolgsfaktor in: Rechts- und Haftungsrisiken im Unternehmensmanagement, hg. von Stefan Hirschmann/Frank Romeike, Köln 2006, S. 86ff.

¹³ Der angelsächsische Ansatz BS 7799 des British Standard Institute (BSI-GB) wurde nach einem Reifeprozess in den Jahren 1993 bis 1997 in zwei Teile aufgespalten. BS 7799 Part 1:2002, Code of Practice for Information Security Management bzw. BS 7799 Part 2:2002, Information Security Management System (ISMS) - Specification with guidance for use.

¹⁴ ISO/IEC 17799:2005, Code of Practice for Information Security Management, bzw. ISO/IEC 27001:2005. Der Teil 1 des BS7799 ist in die ISO/IEC 17799 überführt und im Jahr 2005 novelliert worden. Die aktuelle Version trägt die Bezeichnung ISO/IEC 17799:2005. Die novellierte Version hat einige Verbesserungen u.a. im Outsourcing und im Umgang mit Fremdfirmen erfahren. Diese Norm soll 2007 in die Norm ISO/IEC 27001:2007 unverändert überführt werden. Der Teil 2 des BS7799 ist in die ISO/IEC 27001:2005 überführt worden.

oder dem IT-Grundschutzhandbuch des BSI¹⁵ entsprechen. Andere Beispiele sind die Versionen für Australien und Neuseeland AS/NZS 4444, für Dänemark DS484, Schweden SS627799, die Schweiz SN17799 oder Österreich ÖNORM 17799. Sie stimmen vom Grundsatz her weitgehend überein. Die Verfahren der Zertifizierung sind dagegen z.T. sehr unterschiedlich. Ein nach ISO/IEC 27001 ausgerichtetes ISMS enthält als zentrales Element die Risikoanalyse, die sich mit den kritischen Geschäftsprozessen intensiv auseinandersetzt. Ein solches Element besitzt ein IMS nicht. Als zentrales Element eines IMS kann das für das BS 15000 entwickelte IT-Service Management (ITIL) betrachtet werden. Inzwischen ist auch der Britische Standard (BS) in die beiden internationalen Normen ISO/IEC 2000-1:2005 und ISO/IEC 2000-2:2005 im Jahre 2005 integriert worden. Erst die Entwicklung von Sicherheitspolitiken und Sicherheitsleitlinien zielte somit stärker auf eine umfassendere Betrachtung der IT-Sicherheit bzw. des Managements von IT-Risiken im Unternehmen ab. In einem ISMS sind die Sicherheitsrichtlinien – die Security Policies – von zentraler Bedeutung. Sie enthalten die Festlegungen, die erforderlich sind, um die verschiedenen Systemelemente den Anforderungen anzupassen. Sie legen darüber hinaus die Verantwortlichkeiten für die einzelnen Bereiche fest. Schließlich gibt die Security Policy Regeln für das Verhalten der Mitarbeiter im Umgang mit IT-Systemen vor.

Zwar wird der Begriff der Sicherheitspolitik in der modernen Definition uneinheitlich verwandt, doch kann der Begriff dahingehend eingegrenzt werden, dass Regeln definiert werden, die festlegen, wer mit wem wozu, auf was bezogen und in welcher Art bestimmte Aktivitäten durchzuführen hat¹⁶:

- Entities (Akteure/Objekte)
- Erlaubte Aktivitäten (Aktionen/Beziehungen)
- Sichere Konfigurationen/Vorwarnungen
- Umsetzungen bezüglich Absicherung, Erkennen, Reagieren

Erst das sicherheitstechnische Zusammenspiel, bezogen auf ein vorab definiertes Sicherheitsniveau dieser Komponenten, kann allerdings als IT-Sicherheitsmanagement aufgefasst werden. Als allgemein akzeptierte Komponenten eines IT-Sicherheitsmanagement sind die des BS 7799-1 zu nennen, die wie folgt lauten:

1. Sicherheitspolitiken
2. Organisation der Sicherheitspolitik
3. Einstufung und Kontrolle der Werte
4. Personelle Sicherheit
5. Physische und umgebungsbezogene Sicherheit
6. Management der Kommunikation und des Betriebes
7. Zugangskontrolle
8. Systementwicklung und Wartung
9. Management des kontinuierlichen Geschäftsbetriebes
10. Einhaltung von (gesetzlichen) Verpflichtungen

Auch im IT-GsHB sind diese zehn Normenelemente verankert. Darüber hinaus schlägt das IT-GsHB in Form von Bausteinen bzw. Katalogen konkrete Maßnahmen vor, die gegen dort aufgeführte Gefährdungen wirken. Die Risikoanalyse nach BS 7799 (ISO 27001) ist auf der strategischen Ebene angesiedelt und adressiert Geschäftsprozesse. Dagegen adressiert die Risikoanalyse beim IT-GsHB vornehmlich IT-Komponenten. Zudem verlangt BS 7799 (ISO/IEC 27001) die Durchführung einer individuellen Risikoanalyse, um die Sicherheitsmaßnahmen optimal an die Anforderungen der Geschäftsprozesse anzupassen. Dahingegen liegt dem IT-GsHB eine allgemeine, vom BSI durchgeführte Analyse zu Grunde, die IT-

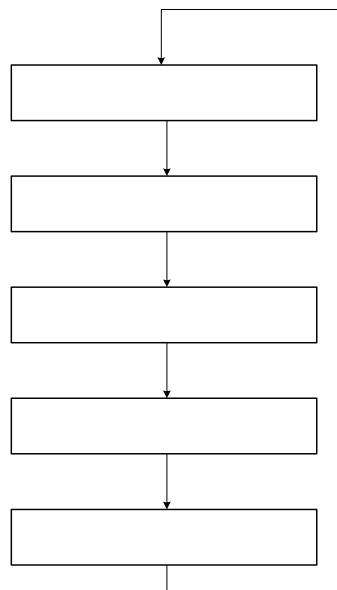
¹⁵ IT-Grundschutzhandbuch: Standard Sicherheitsmaßnahmen, Köln 2004

¹⁶ Zusammenfassend Böhmer, IT-Governance, S. 94ff.

Grundschutz-Maßnahmen mit den im IT-GsHB aufgeführten Bedrohungen in Beziehung setzt¹⁷.

Eine Beurteilung der Risiken innerhalb der Informationssicherheit läuft in der Regel nach einem hierarchischen Schema ab. Dabei wird ein Risikoprozess initiiert, der von der Identifikation von Risiken bis zur Risikokontrolle fünf Schritte durchläuft (Abb. 1). zeigt diese hierarchischen Schritte. Der erste Schritt, die Identifikation sucht in dem Betrachtungsgebiet (Domäne) nach möglichen Risiken. Dabei werden häufig Risiken mit Gefahren gleichgesetzt. Nach einer Identifizierung werden diese analysiert und nachfolgend beurteilt. Die Risikomesung kann zum einen quantitativ oder auch qualitativ vorgenommen werden. Dabei wird bei der quantitativen Messung eine Verbindung zur Eintrittswahrscheinlichkeit gezogen. Bei der qualitativen Messung wird eine Einteilung des Ausmaß: groß, mittel, gering vorgenommen. In der Quantifizierung wird versucht eine monetäre Maßzahl zu finden. Dabei bestimmt der mögliche Schaden die Dimensionseinheit des Risikos. Ist das Risiko beurteilt und quantifiziert, können geeignete Strategien darüber entworfen werden, wie mit dem Gesamtrisiko zu Verfahren ist. Dabei bestehen die grundsätzlichen Möglichkeiten, die identifizierten Risiken selbst zu tragen, zu überwälzen, zu vermindern oder zu vermeiden. Als Restrisiken verbleiben die akzeptierten Risiken und die nicht identifizierten Risiken. Im letzten Schritt erfolgt eine Kontrolle über die Änderungen des Risikozustands¹⁸.

Abbildung 1: Risikoprozess in fünf Schritten



Nach Böhmer, IT-Governance (2006)

5 Anforderungen an ein Informationssicherheitsmanagement

Um eine wirksame Unterstützung im Sinne der Ziele einer IT-Governance zu erreichen, müssen Instrumente geschaffen werden, die eine Führung im Sinne einer kontrollierten Zielerreichung ermöglichen. Welche Richtlinien sind also maßgeblich, um ein effektives Management der Informationssicherheit im Unternehmen zu implementieren?

Wie gesehen, empfiehlt sich als Grundlage der unternehmenseigenen Security Policy die Einrichtung eines anerkannten Standards. Dadurch wird sicher gestellt, dass alle Bereiche in einer übersichtlichen Struktur abgedeckt werden. Selbst wenn im Unternehmen eine Zertifizierung noch nicht angestrebt wird, hilft die Verfolgung eines Standards, zu einem späteren

¹⁷ Ebd.

¹⁸ Vgl. Frank Romeike: IT Risiken und Grenzen traditioneller Risikofinanzierungsprodukte, in: Zeitschrift für Versicherungswesen, 51. Jahrgang, 1. September 2000, Heft 17.

Zeitpunkt kosten- und zeitaufwändige Umstellungen zu vermeiden. Ein zertifiziertes Unternehmen verfügt über entscheidende Vorteile, wie z.B. Business Continuity (Minimierung des Betriebsausfall-Risikos) und dadurch günstigere Versicherungsprämien, die Minimierung des privaten Haftungs-Risikos für Geschäftsführer und Vorstände sowie die Vermeidung strafrechtlicher Risiken. Durch die Zertifizierung wird das Unternehmen im Streitfall in eine verbesserte Position bei arbeitsgerichtlichen Auseinandersetzungen (KSchG und Abfindung) versetzt und erlangt eine bessere Bonität im Kredit-Rating der Banken (Basel II). Zugegeben: Das Erstellen einer ganzheitlichen Unternehmens-Sicherheitsrichtlinie sowie das Umsetzen der sich daraus ergebenden Maßnahmen (ISMS) und die Verankerung im Sicherheitsbewusstsein der Mitarbeiter (Secure Awareness) ist eine recht aufwändige Angelegenheit. Und damit kostenintensiv. Das dürfte auch einer der Gründe dafür sein, dass bisher nur sehr wenige Unternehmen über eine Sicherheitsrichtlinie verfügen. Und dann meist nur bezüglich der Internet-Nutzung oder des E-Mail-Verkehrs. Inzwischen gibt es aber auch schon softwarebasierte Lösungen zur Erstellung, permanenten Aktualisierung und Implementierung einer ganzheitlichen Unternehmens-Sicherheitsrichtlinie, die ISO/IEC 27001-konform ist. So hat die dänische Firma Neupart das Produkt "SecureAware" entwickelt, mit dessen Hilfe eine unternehmensinterne IT-Security Policy erzeugt, im Intranet veröffentlicht werden kann und die sich den individuellen Gegebenheiten des Unternehmens anpassen lässt. Das Produkt erstellt automatisch Wissenstests für die Mitarbeiter. Diese policybezogenen Tests sind eingebunden in Awarenessprogramme (bestehend aus Flash-Filmen, Texten und Wissenstests) zu zehn grundlegenden Sicherheitsthemen. So wird sichergestellt, dass die Mitarbeiter das notwendige Vorwissen haben, um die Policyregeln verstehen zu können.

IT-Security Policy mit fünf Mausklicks

SecureAware entspricht in seinem Aufbau der ISO-Norm 27001, die international verbindliche Empfehlungen zur Realisierung einer ganzheitlichen IT-Sicherheitsrichtlinie liefert. Wer mit unserer Software eine IT-Sicherheitsrichtlinie entwickelt, schafft effektiv und kostengünstig die Grundlage zur Einführung eines ISMS (Information Security Management System). Damit können sich Unternehmen dann nach dem IT-Grundschutzhandbuch des BSI und der ISO-Norm 27001 zertifizieren lassen. Im Ernstfall liefert dies der Führungsebene somit den Nachweis, der Sorgfaltspflicht in der IT-Security nachgekommen zu sein. SecureAware besteht aus drei Teilen, den Modulen Policy, Education und Survey. Zum Paket Policy gehört es firmenspezifische Security-Regeln und -Verfahren zu definieren, zu aktualisieren und an Mitarbeiter zu kommunizieren. Bequem wird das durch eingebaute Vorlagen, die leicht dem individuellen Bedarf angepasst werden können. Mit diesen ISO-Norm-basierten Vorlagen wird insbesondere eine Verwaltung der IT-Unternehmensrichtlinien kosten- und zeiteffizienter. Das film- und sprachunterlegte Education-Softwaremodul ist ein E-Learning-Programm. Es vermittelt Mitarbeitern ein Sicherheits-Grundwissen und gibt Tipps zum richtigen Verhalten im Umgang mit Daten in Hinblick auf die IT-Unternehmenssicherheit. Survey ist ein web-basiertes Testprogramm, mit dem sich das Sicherheitsbewusstsein der Mitarbeiter und der Kenntnisstand der unternehmensspezifischen Sicherheitsrichtlinie überprüfen lässt. Die Inhalte der Tests können auf die unterschiedlichen Gruppen von Mitarbeitern zugeschnitten werden. Kein User muss Regeln lesen und lernen, die nicht zu seinem Aufgabenbereich gehören.
